CLAIMS

What is claimed is:

1. A method for establishing a secure connection to a server for a user of a client computer on a network utilizing a Secure Sockets Layer (SSL) system, said method comprising:

storing a plurality of keyfiles in a data storage accessible to a client computer, each of said keyfiles comprising a unique private cryptology key and a unique digital certificate;

storing a plurality of passwords in said data storage, each of said passwords being associated with a respective keyfile, each of said passwords being capable of opening one of said keyfiles;

in response to receiving one of said passwords input from a user, opening one of said keyfiles associated with said one of said passwords; and

transmitting from said client computer to a server a digital certificate from said open keyfile to enable said server to authenticate an identity of said user.

2. The method of claim 1, further comprising:

storing an authentication data for said user in said data storage, said authentication data comprising a unique identifier that corresponds to a password for said user; and

identifying said user for opening a keyfile according to said unique identifier.

3. The method of claim 1, further comprising:

authenticating an identity of said user through a process of hashing, said process including the steps of:

hashing a message into a hashed message using a hash function;

encrypting said hashed message into an encrypted hashed message using said private cryptology key; and

transmitting said hash function, said message and said encrypted hashed message to said server.

4. The method of claim 1, further comprising prompting said user for a password through a Graphical User Interface (GUI) in a display associated with said client computer.

5. A client computer for establishing a secure connection to a server for a user of the client computer on a network utilizing a Secure Sockets Layer (SSL) system, said client computer comprising:

means for storing a plurality of keyfiles in a data storage accessible to a client computer, each of said keyfiles comprising a unique private cryptology key and a unique digital certificate;

means for storing a plurality of passwords in said data storage, each of said passwords being associated with a respective keyfile, each of said passwords being capable of opening one of said keyfiles;

means for in response to receiving one of said passwords input from a user, opening one of said keyfiles associated with said one of said passwords; and

means for transmitting from said client computer to a server a digital certificate from said open keyfile to enable said server to authenticate an identity of said user.

6. The client computer of claim 5, further comprising:

means for storing an authentication data for said user in said data storage, said authentication data comprising a unique identifier that corresponds to a password for said user; and

means for identifying said user for opening a keyfile according to said unique identifier.

7. The client computer of claim 5, further comprising:

means for authenticating the identity of said user through a process of hashing, said means for authenticating the identity of said user through said process of hashing including:

means for hashing a message into a hashed message using a hash function;

means for encrypting said hashed message into an encrypted hashed message using said private cryptology key; and

means for transmitting said hash function, said message and said encrypted hashed message to said server.

8. The client computer of claim 5, further comprising means for prompting said user for a password through a Graphical User Interface (GUI) in a display associated with said client computer.

9. A computer program product residing on a computer usable medium for establishing a secure connection to a server for a user of a client computer on a network utilizing a Secure Sockets Layer (SSL) system, said computer program product comprising:

program code means for storing a plurality of keyfiles in a data storage accessible to a client computer, each of said keyfiles comprising a unique private cryptology key and a unique digital certificate;

program code means for storing a plurality of passwords in said data storage, each of said passwords being associated with a respective keyfile, each of said passwords being capable of opening one of said keyfiles;

program code means for in response to receiving one of said passwords input from a user, opening one of said keyfiles associated with said one of said passwords; and

program code means for transmitting from said client computer to a server a digital certificate from said open keyfile to enable said server to authenticate an identity of said user.

10. The computer program product of claim 9, further comprising:

program code means for storing an authentication data for said user in said data storage, said authentication data comprising a unique identifier that corresponds to a password for said user; and

program code means for identifying said user for opening a keyfile according to said unique identifier.

11. The computer program product of claim 9, further comprising:

program code means for authenticating the identity of the user through a process of hashing, said program code means including:

program code means for hashing a message into a hashed message using a hash function;

program code means for encrypting said hashed message into an encrypted hashed message using said private cryptology key; and

program code means for transmitting said hash function, said message and said encrypted hashed message to said server.

12. The computer program product of claim 9, further comprising:

program code means for displaying a Graphical User Interface (GUI) in a display associated with said client computer; and

program code means for prompting said user for a password through said GUI.